SYSTEM AND METHOD PROVIDING SECURE ACCESS AND ROAMING SUPPORT FOR MOBILE SUBSCRIBERS IN A SEMI-CONNECTED MODE

FIELD OF THE INVENTION

[0001] The present invention relates to telecommunication systems. More particularly, and not by way of limitation, the invention relates to a system and method for providing secure access and roaming support for mobile subscribers who are connected to a telecommunication network in a Semi-Connected Mode (SCM).

BACKGROUND ART

[0002] In order to access the Internet from a (mobile) phone via an access server, a Point-to-Point Protocol (PPP) connection is established. Negotiation and setup of the PPP connection is conducted in several phases. First, in the Link Control Protocol (LCP) phase, a link is configured. Afterwards, in the Password Authentication Protocol/Challenge Handshake Authentication Protocol (PAP/CHAP) phase, user authentication is performed. Finally, in the network phase, the configuration of the network layer is performed to complete the setup of the PPP connection. For each phase, configuration messages are sent between the mobile phone and the access server. In comparison to the Integrated Services Digital Network (ISDN), negotiation and setup of the PPP connection in mobile networks is quite lengthy due to the relatively long delays of data bearers in wireless networks.

[0003] When a mobile user has no data to transmit for a period of time, it would be useful to temporarily disconnect the call, and then re-establish the call when there is again a need to send data. However, the delay associated with the negotiation and setup of the PPP connection in mobile networks prevents the user from re-establishing the connection in a timely manner. Such a procedure could only be attractive for the user if the delay introduced by the PPP negotiation performed at re-establishment can be shortened.

[0004] A new feature referred to herein as the Semi-Connected Mode (SCM) has been presented to the Internet Engineering Task Force (IETF). Referred to by various other names in the industry, SCM introduces a new state referred to herein as the "Semi-Connected state" to the PPP state machine. The new state allows faster reestablishment of a PPP connection by saving and reusing the parameters that have been hand-shaken in an original, but temporarily disconnected, connection. Simply stated, SCM bypasses the PPP configuration phases by re-using the PPP configuration information of the last session, and utilizing the user's Calling Number Identification (CNID) for authentication.

[0005] FIG. 1 illustrates the PPP state machine 10. From a "Dead" state 11, call setup begins when a link is configured in an "Establish" state 12. Authentication is then performed in an "Authenticate" state 13. If authentication is successful, the PPP state machine moves to a "Network" state 14. When the conncetion is permanently disconnected, the state machine moves to a "Terminate" state 15, and then returns to the Dead state. The connection enters the "Semi-Connected" state 16 when the call is temporarily disconnected after a successful PPP negotiation (i.e., PPP in Network State). The connection will remain in the Semi-Connected state for a predefined wait-time as configured in the access server. If a new call from the same GSM subscriber is received when in the Semi-Connected state, the CNID is used for authenticating the call (i.e., the CNID is checked to determine that the call comes from the same mobile subscriber as the initial call). The connection then returns to the Network state. If no new call is received during the wait-time when in the Semi-Connected state, a timeout occurs, and the state machine returns to the Dead state.

[0006] FIG. 2 is a simplified block diagram of a network PPP connection illustrating a problem that occurs in the prior art when attempting to use SCM with a roaming mobile subscriber. A first call and PPP connection are set up from a mobile station 21 through a first Mobile Switching Center (MSC_1) 22, and a first Access Server (AS_1) 23 to an Internet Protocol (IP) network 24. The call is then temporarily disconnected, moving the connection to the Semi-Connected state. Meanwhile, if the mobile station roams to a new location and attempts to re-establish the call, the second call may be directed to a second MSC (MSC_2) 25 and a second Access Server (AS_2) 26. In this case, AS_2 will not find a cache entry that matches the mobile station's CNID. Therefore, AS_2 treats the call as a new PPP login, and follows the lengthy PPP connection process. Thus, following a temporary disconnection, SCM requires that the subsequent call be placed in the same access server as the first call. To be able to use SCM in such cases, a call would have to be directed towards the old access server, AS_1. This is not possible in most cases, although, if AS_1 is addressed directly in the subsequent call, it is possible for MSC_2 to establish a circuit-switched connection 27 to MSC_1 for redirecting the call to AS_1. However, this results in a waste of the circuit-switched network resources.

[0007] There is also a potential security problem with the prior art SCM method. As noted above, the calling subscriber's CNID is used to authenticate the subsequent calls when SCM is used. In some cases, however, the CNID does not uniquely identify the calling subscriber. For example, in the case of a call originated from a private branch exchange (PABX) by Primary Rate Access (PRA), the group number may be used as the calling party number. Therefore, all the extensions belonging to the PABX will send the same calling party number, and anyone originating a call from the PABX will be reconnected to the established call.

[0008] Thus, there is a need for a system and method for providing secure access and roaming support for mobile subscribers who are connected to a telecommunication network in the Semi-Connected Mode (SCM). The present invention provides such a system and method.

SUMMARY OF THE INVENTION

[0009] In one aspect, the present invention is directed to a method of providing secure access and roaming support for a mobile subscriber connected to a telecommunication network in a Semi-Connected Mode (SCM). The method includes the steps of establishing a first call from the mobile subscriber to a first access server, and establishing a point-to-point protocol (PPP) connection from the mobile subscriber to an Internet Protocol (IP)-based network through the first access server. The first access server then provides the mobile subscriber with an identifier for the first access server. Optionally, for cases in which the CNID of the mobile subscriber does not uniquely identify the subscriber (for example the CNID is a group number from a PABX), AS_1 may also provide the subscriber with a password that uniquely identifies the client. The password is stored in AS_1 and is accessible using the CNID for the calling subscriber as a lookup key. When the mobile subscriber disconnects the first call, the connection moves to the SCM state. This is followed by receiving from the mobile subscriber, the identifier for the first access server. The identifier is received in a second access server that handles a subsequent call origination from the mobile subscriber to the IP-based network. The second access server utilizes the identifier for the first access server to send a Calling Number

Identification (CNID) for the mobile subscriber from the second access server to the first access server. This is followed by establishing a PPP tunnel through the IP-based network between the first access server and the second access server; tunnelling PPP packets from the second access server to the first access server; and re-establishing the connection from the mobile subscriber to the IP-based network.

[0010] In another aspect, the present invention is directed to a method of providing secure access and roaming support for a mobile subscriber connected to a telecommunication network in an SCM state. The method includes the steps of establishing a first call from the mobile subscriber to a first access server, and establishing a PPP connection from the mobile subscriber to an IP-based network through the first access server. The first access server then provides the mobile subscriber with an identifier for the first access server. When the mobile subscriber disconnects the first call, the connection moves to the SCM state. This is followed by receiving from the mobile subscriber, the identifier for the first access server. The identifier is received in a second access server that handles a subsequent call origination from the mobile subscriber to the IP-based network.

[0011] The second access server analyzes the identifier for the first access server to determine whether the second access server is the first access server. If the second access server is the first access server, the access server determines whether it recognizes the CNID for the mobile subscriber. If the CNID is recognized, the access server re-establishes the connection from the mobile subscriber to the IP-based network. If the CNID is not recognized, the access server starts a new PPP setup to establish a new connection from the mobile subscriber to the IP-based network. However, if the second access server is not the first access server, the second access server sends the CNID for the mobile subscriber to the first access server. The first access server then determines whether it recognizes the CNID for the mobile subscriber. If the CNID is recognized, the first access server uses the CNID to look up SCM data for the connection. A PPP tunnel is then established through the IP-based network between the first access server and the second access server, and PPP packets are tunnelled from the second access server to the first access server. The connection from the mobile subscriber to the IP-based network is then re-established. If the CNID is not recognized, the first access server sends a negative reply to the second access server. The second access server then starts a new PPP setup to establish a new connection from the mobile subscriber to the IP-based network.

[0012] In yet another aspect, the present invention is directed to a system for providing secure access and roaming support for a mobile subscriber connected to a telecommunication network in an SCM state. The system includes a first access server that establishes a call and a PPP connection from the mobile subscriber to an IP-based network; a second access server that handles a subsequent call origination from the mobile subscriber to the IP-based network; and a PPP tunnel between the first access server and the second access server. The first access server includes communication means for providing the mobile subscriber with an identifier for the first access server; and means controlled by a PPP state machine for placing the connection in a Semi-Connected state when the mobile subscriber disconnects the call, and for placing the connection in a Network state when the mobile subscriber originates the subsequent call origination. The second access server includes communication means for receiving the identifier for the first access server from the mobile subscriber, and for sending the CNID for the mobile subscriber from the second access server to the first access server. The second access server also includes means for tunnelling PPP packets from the second access server to the first access server through the PPP tunnel. In this manner, the connection from the mobile subscriber to the IP-based network is re-established.

[0013] In still yet another aspect, the present invention is directed to a network access server for providing secure access and roaming support for a mobile subscriber connected to a telecommunication network in an SCM state. The network access server includes means for receiving a call origination request from the mobile subscriber that includes a CNID for the mobile subscriber; means for establishing a PPP connection from the mobile subscriber to the network; and means for providing the mobile subscriber with an identifier for the network access server. The network access server also includes means for storing SCM data for the connection and moving the connection to the SCM state when the mobile subscriber disconnects from the network access server; means for receiving from a subsequent access server, the CNID of the mobile subscriber when the mobile subscriber originates another call request through the subsequent access server; and means for retrieving the SCM data using the CNID of the mobile subscriber. The network access server also includes means for setting up a PPP tunnel through the network to the subsequent access server. The PPP tunnel re-establishes the connection from the mobile subscriber to the network by tunnelling PPP packets from the subsequent access server to the network access server without establishing a new PPP connection.

[0014] In still yet another aspect, the present invention is directed to a network access server for providing secure access and roaming support for a mobile subscriber connected to a telecommunication network in an SCM state. The network access server includes means for receiving a call origination request from the mobile subscriber that includes a CNID for the mobile subscriber and an identifier for a previous access server through which a PPP connection was previously established from the mobile subscriber to the network. The network access server also includes means for sending the CNID for the mobile subscriber to the previous access server and means for setting up a PPP tunnel through the network to the previous access server in response to a request from the previous access server. The PPP tunnel re-establishes the connection from the mobile subscriber to the network by tunnelling PPP packets from the network access server to the previous access server without establishing a new PPP connection.

BRIEF DESCRIPTION OF THE DRAWINGS

[0015] In the following section, the invention will be described with reference to exemplary embodiments illustrated in the figures, in which:

[0016] FIG. 1 (Prior Art) illustrates a Point-to-Point Protocol (PPP) state machine;

[0017] FIG. 2 (Prior Art) is a simplified block diagram of a network PPP connection illustrating a problem that occurs in the prior art when attempting to use SCM with a roaming mobile subscriber;

[0018] FIG. 3 is a simplified block diagram of a network PPP connection illustrating the preferred embodiment of the system of the present invention when using SCM with a roaming mobile subscriber; and

[0019] FIG. 4 is a flow chart illustrating the steps of the preferred embodiment of the method of the present invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

[0020] In the following description, for purposes of explanation and not limitation, specific details are set forth, such as particular embodiments, circuits, signal formats etc. in order to provide a thorough understanding of the present invention. It will be apparent to one skilled in the art that the present invention may be practiced in other embodiments that depart from these specific details.

[0021] FIG. 3 is a simplified block diagram of a network PPP connection illustrating the preferred embodiment of the system of the present invention when using SCM with a roaming mobile subscriber. As utilized in the present invention, SCM provides a way to reduce the PPP setup delay, and therefore increase available radio resources and decrease costs for data transmission. When setting up an initial call, if the calling subscriber 21 wants to use the SCM, the client (e.g., mobile phone) of the calling subscriber may send a request for SCM to the first access server (AS_1) 23. If SCM is applicable for the call, AS_1 replies to the request and provides to the client an identifier of AS_1. The identifier may be, for example, an IP address of AS_1 that identifies AS_1 in the IP network 24. Optionally, for cases in which the CNID of the client does not uniquely identify the client (for example the CNID is a group number from a PABX), AS_1 may also provide the client with a password that uniquely identifies the client. The password is stored in AS_1 and is accessible using the CNID for the calling subscriber as a lookup key. AS_1 considers the CNID as the user-id to be used for login. The SCM request and reply exchanged between the client and AS_1 may be sent utilizing a vendor-specific extension in the PPP protocol or with IP packets. It should be recognized that the identifier of AS_1 and the password may also be sent without an explicit request from the client if, for example, the subscriber is marked as an SCM subscriber.

[0022] When the calling subscriber roams and originates a subsequent call, the client provides the access server of the subsequent call (AS_2) 26 with the identifier of AS_1 23 (and optionally the password), which was received when setting up the initial call. The identifier may be sent using the PPP protocol, but is preferably sent to AS_2 utilizing the User-to-User Signalling (UUS) Supplementary Service. The UUS Supplementary Service is a standard GSM signalling method that enables users to exchange a limited amount of information between each other. The information is passed transparently through the network. Advantageously, UUS signalling is performed before a call is established (i.e., before an answer message is sent), and before PPP setup of the connection is started. In addition, a tunnel using the Layer 2 Tunnelling Protocol (L2TP) may also be set up in advance, before the connection is established. The UUS Supplementary Service is described in GSM 2.87 User to User Signalling (UUS) Service description stage 1; GSM 3.87 User to User Signalling (UUS) Supplementary Service Stage 2; GSM 4.87 User to User Signalling (UUS) Supplementary Service Stage 3; and the ISDN Supplementary Service ETSI UUS Stage 3, prETS 300 286, Dec. 1995, all of which are hereby incorporated by reference herein.

[0023] AS_2 26 uses the identifier of AS_1 23 to send the CNID of the calling subscriber to AS_1. If a password is also sent, AS_1 uses the CNID to look up and verify the password. A PPP tunnel 28 is then established through the IP network 24 between AS_1 and AS_2. AS_2 then uses the tunnel to send PPP packets to AS_1, and the connection is re-established.

[0024] FIG. 4 is a flow chart illustrating the steps of the preferred embodiment of the method of the present invention. At step 31, the calling subscriber client originates a first call and sends an SCM request to AS_1. At step 32, AS_1 verifies that the client is authorized to use SCM and returns an identifier of AS_1 such as AS_1's IP address to the client. At step 33, the PPP state then moves to Network, and the connection is established. At step 34, the client temporarily disconnects the call, and the PPP state of the connection moves to Semi-Connected at step 35.

[0025] The client may then roam to another location, which may or may not be served by AS_1, and at step 36, originates a subsequent call. The client sends the IP address of AS_1 to the access server that is serving the subsequent call (AS_{SUB}). At step 37, AS_{SUB} determines whether it is AS_1 by analyzing the IP address sent by the client. If AS_{SUB} is AS_1, the method moves to step 38 where AS_1 determines whether the CNID of the calling subscriber is recognized. If the CNID is not recognized, the method moves to step 39 where AS_1 begins a new PPP setup. However, if the CNID is recognized at step 38, the method moves to step 40 where AS_1 uses the CNID of the calling subscriber to look up the SCM data from the initial connection. At step 41, the PPP state moves to Network, and the connection is re-established at step 42.

[0026] However, if at step 37 it is determined that AS_{SUB} is not AS_1, the method moves from step 37 to step 43 where AS_{SUB} sends the CNID of the calling subscriber to AS_1 using the IP address supplied by the client. At step 44, AS_1 determines whether the CNID of the calling subscriber is recognized. If the CNID is not recognized, the method moves to step 45 where AS_1 sends a negative reply to AS_{SUB}. At step 46, AS_{SUB} begins a new PPP setup. However, if the CNID is recognized at step 44, the method moves to step 47 where AS_1 uses the CNID of the calling subscriber to look up the SCM data from the initial connection. At step 48, a PPP tunnel is established through the IP network between AS_1 and AS_{SUB}. At step 49, AS_{SUB} then tunnels PPP packets to AS_1. At step 50, the PPP state moves to Network, and the connection is re-established at step 51.

[0027] While the present invention has been described with respect to particular embodiments, those skilled in the art will recognize that the present invention is not limited to the specific embodiments described and illustrated herein. Therefore, while the present invention has been described in relation to its preferred embodiments, it is to be understood that this disclosure is only illustrative in nature. Accordingly, it is intended that the invention be limited only by the scope of the claims appended hereto.